Особенности правового регулирования биометрических персональных данных

М.С. Кривогин

аспирант Международной лаборатории по праву информационных технологий и интеллектуальной собственности Национального исследовательского университета «Высшая школа экономики». Адрес: 101000, Российская Федерация, Москва, ул. Мясницкая, 20. E-mail: mkrivogin@yandex.ru

Аннотация

В статье анализируется соотношение правового регулирования специальной и биометрической категорий персональных данных. Выявляется ряд отличительных критериев, на основе которых строится разграничение между названными категориями. Рассматривается проблема осуществления обработки биометрических персональных данных, сделанных общедоступными субъектом персональных данных. Проведено исследование российской и зарубежной доктрины, нормативно-правовых актов, отечественной судебной практики в области правового регулирования различных категорий персональных данных. Сравниваются перечни сведений, составляющих содержание специальной и биометрической категорий персональных данных и возможность обработки таких сведений без согласия субъекта персональных данных. Анализ показывает, что, несмотря на наличие в доктрине и законах многих стран множественности подходов к регулированию биометрических персональных данных, выделение в российском законодательстве биометрической информации в отдельную категорию персональных данных является целесообразным и обоснованным. Основным отличием биометрической категории от специальной категории персональных данных, помимо различных целей их введения в законодательство — запрета дискриминации и ограничения возможности идентификации субъекта, также является и перечень случаев, при которых обработка персональных данных может осуществляться без согласия гражданина. Недопустимость обработки биометрических персональных данных, сделанных общедоступными субъектом персональных данных без его согласия в письменной форме, позволяет обеспечить защиту сведений, контроль над распространением которых субъектом проблематичен. Биометрические персональные данные являются единственным исключением из объективного подхода, который используется при отнесении информации к категории персональных данных. Использование субъективного подхода при обработке биометрических персональных данных позволяет более точно произвести разделение между различными категориями персональных данных. Информация о гражданине будет признана биометрическими персональными данными, если она используется оператором для установления личности субъекта персональных данных. Применение данного подхода в настоящее время позволяет учитывать как интересы субъекта, так и оператора персональных данных.

Ключевые слова

персональные данные, категории персональных данных, биометрические, специальные, общедоступные, Европейский Союз, субъективный подход, объективный подход.

Библиографическое описание: Кривогин М.С. Особенности правового регулирования биометрических персональных данных // Право. Журнал Высшей школы экономики. 2017. № 2. С. 80–89.

JEL: K 24; УДК: 340 DOI: 10.17323/2072-8166.2017.2.80.89

Широкое распространение биометрических технологий пришлось на начало первого десятилетия XXI века и было связано с возрастающей угрозой проведения террористических актов во многих странах мира[1]. Биометрические технологии используются для идентификации субъектов по таким физиологическим, биологическим и поведенческим характеристикам, как геометрия лица, отпечатки пальцев, ДНК, манера ходьбы[2]. Названные характеристики непосредственно относятся к физическим лицам и в большинстве случаев являются персональными данными, при обработке которых применяются положения соответствующего законодательства.

Ко времени массового распространения биометрических технологий в большинство стран Совета Европы уже ратифицировало Конвенцию № 108 «О защите физических лиц при автоматизированной обработке персональных данных» (1981)[3], а страны, входящие в Европейский Союз — Директиву 95/46/ЕС от 24.10.1995 «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных»[4]. Их принятие было направлено на защиту прав граждан при обработке персональных данных, которые в зависимости от степени чувствительности подразделяются на две категории — обычные и специальные. Такое разделение в дальнейшем было воспринято многими странами мира и стало использоваться в национальных нормативно-правовых актах как образец надлежащего учета интересов субъектов персональных данных.

Только несколько стран, включая Италию (2003)[5], Словению (2004)[6] и Россию (2006)[7], внесли в законодательство обособленное регулирование для биометрических персональных данных еще до появления судебной практики в данной сфере.

Необходимость и целесообразность введения специального регулирования новых категорий персональных данных зачастую вызывает обоснованные сомнения в научной литературе. По мнению канадского исследователя Ю. Лиу, такое выделение не является целесообразным, поскольку существующее регулирование обработки персональных данных обеспечивает адекватную защиту прав субъектов[8]. В европейской доктрине, наоборот, существует тенденция к повышению уровня защиты прав граждан в сфере обработки персональных данных. Так, в рекомендательных документах рабочей группы ЕС в сфере защиты прав граждан при обработке персональных данных указано на допустимость внесения в законодательство дополнительных категорий персональных данных после надлежащего определения предмета регулирования в данной сфере[9].

---

[1] *Kittichaisaree K.* Public International Law of Cyberspace. Bern, 2017. P. 65.

[2] *Mordini E.* Second Generation Biometrics: The Ethical, Legal and Social Context. N.Y., 2012. P. 130.

[3] Конвенция о защите физических лиц при автоматизированной обработке персональных данных (заключена в Страсбурге 28.01.1981) // СПС КонсультантПлюс.

[4] Директива N 95/46/ЕС Европейского парламента и Совета Европейского Союза «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных» (принята в Люксембурге 24.10.1995) (с изм. и доп. от 29.09.2003) // СПС КонсультантПлюс.

[5] Data Protection Code — Legislative Decree no. 196/2003 [Электронный ресурс]: // URL: http://194.242.234.211/web/guest/home/docweb/-/docweb-display/docweb/4814258 (дата обращения: 18.07.2016)

[6] Personal Data Protection Act of the Republic of Slovenia No. 001-22-148/04 [Электронный ресурс]: // URL: https://www.coe.int/t/dghl/standardsetting/dataprotection/National%20laws/SLOVENIA_DP_LAW.pdf (дата обращения: 19.07.2016)

[7] Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных» // СЗ РФ. № 31. Ст. 3451.

[8] *Yue Liu N.* Bio-Privacy: Privacy Regulations and the Challenge of Biometrics. N. Y., 2012. P. 151.

[9] Advice Paper on Special Categories of Data («Sensitive Data»). [Электронный ресурс]: // URL: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/others/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf (дата обращения: 19.07.2016)

Е. Киндт, автор одного из немногочисленных исследований в сфере правового регулирования обработки биометрических персональных данных в ЕС, указывает на необходимость скорейшего выделения дополнительных категорий, поскольку при отнесении биометрической информации к обычной категории персональных данных не происходит учета особенностей данного вида сведений, создаются существенные угрозы нарушения прав субъектов[10].

В отечественных научных работах не существует единства мнений по вопросу выделения биометрической информации из специальной категории персональных данных. Е. Покаместова считает, что наличие специальных норм, регулирующих обработку биометрических персональных данных в российском законодательстве не может считаться обоснованным, поскольку «представляется более логичным относить биометрические персональные данные к одному из видов специальных категорий персональных данных»[11]. И. Вельдер, наоборот, ссылаясь на активное использование биометрических персональных данных, говорит о необходимости правового регулирования порядка их сбора и обработки[12]. Также иногда происходит смешение понятия специальной и биометрической категорий персональных данных. Например, в учебнике информационного права под редакцией И.М. Рассолова биометрические персональные данные рассматриваются в качестве входящих в специальную категорию персональных данных[13].

Таким образом, как в российской, так и зарубежной доктрине не существует однозначной позиции о целесообразности выделения биометрических информации в отдельную категорию персональных данных. Несмотря на то, что в российском законодательстве существует отдельная статья, регламентирующая особенности обработки биометрических персональных данных, в нее было внесено множество поправок[14], и новые законопроекты продолжают поступать[15].

Причины закрепления в законодательстве о персональных данных специальных и биометрических категорий различны. Перечень информации, относящейся к специальной категории персональных данных во многом совпадает со ст. 14 Европейской конвенции о защите прав человека и основных свобод (1950): раса, религия, политические и иные убеждения, национальное происхождение[16]. Основной целью включения такой информации в список чувствительных персональных данных изначально (в рамках

---

[10] *Kindt E.* Privacy and Data Protection Issues of Biometric Applications. Leyden, 2013. P. 745.

[11] *Покаместова Е.Ю.* Правовая защита конфиденциальности персональных данных несовершеннолетних: дис. … к.ю.н. Воронеж, 2006. С. 51.

[12] *Вельдер И.А.* Система правовой защиты персональных данных в Европейском Союзе: дис. … к.ю.н. Казань, 2006. С. 131.

[13] *Рассолов И.М.* Информационное право. М.: Юрайт, 2012. С. 165–166.

[14] Федеральный закон от 25.11.2009 № 266-ФЗ «О внесении изменений в Федеральный закон «О персональных данных» по вопросам реализации международных договоров Российской Федерации о реадмиссии» // СЗ РФ. № 48. Ст. 5716; Федеральный закон от 25.07.2011 №261-ФЗ «О внесении изменений в федеральный закон «О персональных данных» // СЗ РФ. № 31. Ст. 4701; Федеральный закон от 04.06.2014 № 142-ФЗ «О внесении изменений в статьи 6 и 30 Федерального закона «О гражданстве Российской Федерации» и отдельные законодательные акты Российской Федерации» // СЗ РФ. № 23. Ст. 2927.

[15] Законопроект № 416052-6 о внесении изменений в Федеральный закон «О персональных данных» и статью 28.3 Кодекса Российской Федерации об административных правонарушениях. [Электронный ресурс]: // URL: http://asozd2.duma.gov.ru/main.nsf/(Spravka)?OpenAgent&RN=416052-6&11 (дата обращения: 15.07.2016)

[16] Конвенция о защите прав человека и основных свобод (заключена в Риме 04.11.1950) // СПС КонсультантПлюс.

Конвенции Совета Европы № 108 «О защите физических лиц при автоматизированной обработке персональных данных», а также в ФЗ Российской Федерации от 27.07.2006 «О персональных данных») было предоставление гражданам дополнительных гарантий от дискриминации в условиях применения информационных технологий при обработке информации. Это зачастую обуславливалось печальным опытом использования таких сведений и технологий их обработки в тоталитарных государствах[17]. В дальнейшем с появлением Интернета, происходит частичное изменение сущности такой информации; помимо запрета дискриминации также важную роль начинает играть режим конфиденциальности информации, когда доступ к таким сведениям третьих лиц помимо воли субъекта уже означает существенное нарушение его прав[18].

Биометрические сведения также могут использоваться в целях дискриминации; например, информация, содержащаяся в ДНК, позволяет установить предрасположенность индивида к определенным заболеваниям, что впоследствии может быть использовано в сфере трудоустройства, страхования и т.п.[19] Однако указанные сведения уже отнесены к специальной категории персональных данных, а именно, к информации о здоровье. Аналогичное регулирование применяется и при автоматизированной обработке информации о расовой принадлежности субъекта, и, несмотря на то, что в такой ситуации могут использоваться биометрические технологии, обработка указанных данных будет также относиться к положениям о защите информации, относящейся к специальной категории персональных данных.

В данном случае чувствительность биометрических персональных данных обуславливается их свойствами. Во-первых, биометрические характеристики являются уникальными и универсальными например, ДНК, отпечатки пальцев, геометрия лица (в большинстве случаев) присущи исключительно одному человеку, что позволяет осуществить идентификацию физического лица и существенно ограничивать право на неприкосновенность частной жизни. Во-вторых, такая информация, а также содержащие ее материальные носители становятся доступны для сбора и анализа другим лицам в процессе повседневной активности субъекта, независимо от его воли, что дает возможность производить накопление и обработку таких сведений скрытно, без уведомления субъекта. В-третьих, в отличие от других персональных данных, например, фамилии, имени, которые присваиваются другими субъектами или государством и могут быть в дальнейшем изменены, биометрические характеристики являются практически неизменяемыми, что может привести к негативным последствиям в случае неправомерного их использования третьими лицами. Аналогично использование биометрических данных в криминалистических целях, их распространенность и трудность доказывания невиновности в случае обнаружения на месте преступления отпечатков пальцев или биологического материала подозреваемого также говорит о чувствительности данных сведений[20].

В связи с этим права, которые гарантированы законодательством в сфере защиты персональных данных, например, право субъекта на доступ к своим персональным

---

[17] *Black E.* IBM and Holocaust: Strategic Alliance between Nazi Germany and America's Most Powerful Corporation. N. Y., 2012. P. 15.

[18] *Kindt E.* Op. cit. P. 132.

[19] *Gkoulalas-Divanis A.* Medical Data Privacy Handbook. Berlin, 2015. P. 619.

[20] *Горелишвили Д.* Постатейный комментарий к проекту Закона России «О персональных данных». [Электронный ресурс]: // URL: http://www.kongord.ru/Index/A_tma_05/DGorpersdatcom.html (дата обращения: 16.07.2016)

данным, возможность получения информации об операторе и уведомления о начале обработки не всегда могут быть осуществлены, что также делает декларативным право субъекта на возражение против использования его персональных данных.

Приведенные выше обстоятельства позволяют рассматривать биометрические персональные данные в качестве чувствительной информации, обработка которой должна регулироваться специальными нормами. Это подтверждается также и моделями зарубежного законодательства, где биометрическая информация рассматривается в качестве чувствительных сведений в рамках законодательства о защите персональных данных Чехии[21], Италии[22], Эстонии[23], Франции[24].

Несмотря на то, что биометрические персональные данные относятся к чувствительной информации, что предполагает специальные правила их обработки, применяемое регулирование может не соответствовать особенностям данной информации, и поэтому выделение «сверхчувствительных» сведений в отдельную категорию персональных данных будет являться целесообразным. Такое разделение в настоящее время существует в российском законодательстве. Необходимость внесения в законодательство дополнительной категории персональных данных также определяется отсутствием внутреннего единства в существующих категориях персональных данных, а также высокой вероятностью нарушения прав граждан и их законных интересов при применении общего правового регулирования.

Если рассматривать правовое регулирование сведений, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъекта в рамках специальной категории персональных данных, можно заметить сомнительность применения некоторых положений, касающихся возможности обработки таких сведений без согласия субъекта для указанных видов персональных данных.

Например, обработка информации о политических взглядах гражданина может осуществляться без его согласия в медико-профилактических целях, или в целях установления медицинского диагноза. Аналогично можно сказать и про сведения, касающиеся расовой принадлежности субъекта либо его философских убеждений, и про обработку таких данных, осуществляемой в соответствии с пенсионным или страховым законодательством. Список приведенных примеров не является исчерпывающим, его можно продолжить, однако в этом нет необходимости, поскольку цель таких примеров — показать отсутствие единства между всей совокупностью сведений, входящих в специальную категорию персональных данных и коллизиями при обработке указанных сведений без согласия субъекта персональных данных. Исходя из этого, тезис о том, что отдельные положения, которые применимы к специальным категориям персональных данных, могут не полностью соответствовать характеру биометрической информации,

---

[21] Act No. 101/2000 Coll. On the Protection of Personal Data. Czech Republic. [Электронный ресурс]: // URL: https://www.uoou.cz/en/vismo/zobraz_dok.asp?id_ktg=1107 (дата обращения: 18.07.2016)

[22] Data Protection Code — Legislative Decree of Italy No. 196/2003. [Электронный ресурс]: // URL: http://194.242.234.211/web/guest/home/docweb/-/docweb-display/docweb/4814258 (дата обращения: 18.07.2016)

[23] Personal Data Protection Act No RT 127 of 15 February 2007 [Электронный ресурс]: // URL: https://www.riigiteataja.ee/en/eli/ee/529012015008/consolide/current (дата обращения: 18.07.2016)

[24] Act No 78-17 of 6 January 1978 On Information Technology, Data Files and Civil Liberties. [Электронный ресурс]: // URL: https://www.cnil.fr/sites/default/files/typo/document/Act78-17VA.pdf (дата обращения: 18.07.2016)

не находит подтверждения, поскольку даже в категории специальных персональных данных отсутствует внутреннее единство насчет критерия возможности обработки персональных данных без согласия субъекта.

Однако если специальные категории не обладают внутренним единством, то включение в их состав биометрической информации существенным образом ни на что не повлияет. В то же время из сопоставления примеров разрешенного использования персональных данных, относящихся к биометрической или специальной категории без согласия субъекта, можно выделить два существенных отличия. Во-первых, это обработка персональных данных, которые были сделаны общедоступными субъектом персональных данных, во-вторых, это обработка персональных данных, которая необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных либо жизни, здоровья или иных жизненно важных интересов других лиц, получение же согласия субъекта персональных данных невозможно.

Наиболее значимым в контексте биометрии является первый фактор, когда независимо от того, были ли сделаны биометрические персональные данные публичными, оператор должен получить от субъекта согласие на их обработку. Несмотря на то, что данная норма существовала в первой редакции ФЗ «О персональных данных» еще в 2006 году, она опередила свое время, и сегодня, с учетом технического прогресса, особенно в сфере распознавания изображений, является весьма актуальной.

В 2006 году социальные сети не имели столь широкого охвата аудитории, который они имеют в настоящее время: в глобальном масштабе количество пользователей Facebook составляло 12 млн. человек[25], Vkontakte — несколько тысяч[26]. В дальнейшем в социальных сетях многократно увеличивается число пользователей и количество загружаемых данных, которые в большинстве представлены фотографиями физических лиц.

Практически все социальные сети устанавливают правила обработки персональных данных, с которыми пользователь соглашается при регистрации, где ввиду отсутствия ограничений в настройках конфиденциальности на доступ к данным сведениям третьих лиц, персональные данные будут считаться сделанными общедоступными субъектом персональных данных с позиции п. 10 ч. 1 ст. 6 и п. 2 ч. 2 ст. 10 ФЗ «О персональных данных»[27].

Поскольку изображение на странице пользователя является персональными данными, которые были сделаны общедоступными, другие лица могут обрабатывать соответствующую информацию без согласия субъекта. В большинстве случаев такая обработка сводится к размещению фотографии на других страницах социальной сети или других сайтах в Интернете. Однако применение такого варианта регулирования к биометрическим персональным данным применение такого регулирования могло бы оказать негативное влияние на права субъекта. Делая собственные персональные данные общедоступными, субъект не может предвидеть, что новые информационные технологии будут изменять самую сущность использования такой информации: вместо распространения — возможность автоматизированной идентификации человека любыми субъектами, когда лицо становится универсальным идентификатором.

---

[25] *Gregory M.* Security and the Networked Society. London, 2013. P. 248.

[26] [Электронный ресурс]: // URL: https://ru.wikipedia.org/В Контакте (дата обращения: 17.07.2016)

[27] Правила защиты информации о пользователях сайта VK.com17. [Электронный ресурс]: // URL: https://new.vk.com/privacy (дата обращения 17.07.2016); Что считается общедоступной информацией? [Электронный ресурс]: // URL: https://www.facebook.com/help/203805466323736 (дата обращения 17.07.2016)

Даже если субъект придает важное значение распространяемой о себе информации в Интернете, не размещая ее в общедоступных источниках персональных данных, либо не делая ее общедоступной, тем не менее он не в состоянии полностью ограничить ее обработку. Например, обнародование изображения гражданина в Интернете допускается без его согласия, если оно было получено в открытых для свободного посещения местах и не является основным объектом использования (пп. 2 п. 1 ст. 152.1 ГК РФ).

Приведенные обстоятельства существенно уменьшают возможность контроля субъекта над использованием его персональных данных, поэтому рациональным шагом было установление дополнительных ограничений для других лиц при использовании ими персональных данных, которые были сделаны общедоступными субъектом. Однако это не означает, что обработка сведений, сделанных общедоступными субъектом персональных данных, должна быть полностью запрещена, — для того, чтобы она была легитимной, необходимо согласие субъекта, которое должно выражать его волю, в данном случае именно на обработку биометрических персональных данных. Таким образом, с учетом свойств биометрической информации, а также возможных негативных последствий для субъекта персональных данных происходит изменение в регулировании общедоступных персональных данных — вместо свободы обработки по умолчанию на необходимость получить согласие гражданина.

В связи с развитием информационных технологий, увеличением количества обрабатываемых о гражданах сведений, а также различным идентифицирующим потенциалом данной информации в научной литературе возникает спор о необходимости использования объективного или субъективного подхода при обработке персональных данных[28]. Объективный подход предполагает, что информация признается персональными данными независимо от наличия у оператора возможности произвести идентификацию субъекта[29]. Субъективный подход предполагает, что оператор должен иметь разумную возможность идентифицировать субъекта на основании имеющихся у него дополнительных сведений или той информации, которую он может получить от других лиц[30].

Применительно к специальной и биометрической категориям персональных данных данный подход трансформируется в необходимость установления цели обработки оператором соответствующих сведений. При обработке персональных данных субъекта, например, его фотографии, если исходить из буквального толкования закона, оператор также будет обрабатывать и сведения, относящиеся к специальной категории персональных данных, поскольку изображение лица характеризует расу субъекта, а также может отражать его состояние здоровья. Такой формальный подход подвергся обоснованной критике рядом авторов ввиду отсутствия у оператора знания того, обработку какого типа персональных данных он производит[31].

---

[28] CJEU Decision on Dynamic IP Addresses Touches Fundamental DP Law Questions. [Электронный ресурс]: // URL: https://www.twobirds.com/en/news/articles/2016/global/cjeu-decision-on-dynamic-ip-addresses-touches-fundamental-dp-law-questions (дата обращения: 15.01.2017)

[29] *Cooper D.* Re-defining «Personal Data» — Can the Opinion Live up to the Hype? // Data Protection Ireland. 2016. Vol. 3. Issue 6. P. 7.

[30] *Vermeulen G., De Bondt V.* Justice, Home Affairs and Security: European and International Institutional and Policy Development. Utrecht, 2017. P. 101.

[31] *Simits S.* Revisiting Sensitive Data [Электронный ресурс]: // URL: https://www.coe.int/t/dghl/standardsetting/dataprotection/Reports/Report_Simitis_1999.pdf (дата обращения: 17.07.2016); *McCullagh K.* Data Sensitivity: Proposals for Resolving the Conundrum // Journal of International Commercial Law and Technology. 2007. Issue 4. P. 197.

Биометрические персональные данные являются единственным исключением из объективного подхода к обработке персональных данных в российском законодательстве — они будут относиться к данной категории только если происходит их использование оператором в целях определения личности субъекта.

В отечественном законодательстве более пяти лет существовал объективный подход в отношении обработки биометрических персональных данных, чтобы сведения могли относиться к биометрическим данным, было достаточно, чтобы сведения характеризовали физиологические особенности человека и на основании их можно было установить личность субъекта. Однако применение объективного подхода показало нецелесообразность, поскольку большей частью к обработке биометрических персональных данных относилось либо хранение бумажных копий паспортов клиентов или сотрудников организации[32], либо размещенные материалы с фотографией лица на сайте в Интернете, где данное регулирование в большей степени использовалось для ограничения свободы слова[33]. С внесением поправок в ФЗ «О персональных данных» в 2011 году[34] названные недостатки законодательства были исправлены, и для биометрической категории персональных данных был установлен субъективный подход, т.е. персональные данные будут считаться биометрическими только в случае наличия цели у оператора осуществлять их обработку для идентификации граждан.

Целесообразность применения данного регулирования подтверждается и аналогичными разработками в рамках Общеевропейского регламента о персональных данных № 2016/679 (который заменит национальные нормативно-правовые акты стран ЕС в данной сфере), где также используется субъективный подход для правового регулирования биометрических персональных данных, — биометрические персональные данные будут относиться к специальной категории только при условии, если они используются оператором в целях идентификации физических лиц (ч. 1 ст. 9)[35]. Схожие нормы содержатся и в Директиве ЕС № 2016/680, положения которой применяются в сфере обработки персональных данных компетентными государственными органами в целях предотвращения и расследования преступлений (ст. 10)[36].

Таким образом, выделение биометрической информации в отдельную категорию персональных данных позволяет учесть ее свойства и особенности, а также установить правовое регулирование, учитывающее как интересы субъекта, так и оператора персональных данных.

Библиография

Вельдер И.А. Система правовой защиты персональных данных в Европейском Союзе: дис. … к.ю.н. Казань, 2006. 165 с.

[32] Постановление Фрунзенского районного суда Владивостока от 17.10.2011 по делу 5-143/11; Постановление Ленинского районного суда Тюмени от 15.05.2013 по делу № 5-3642.

[33] Решение по административному делу г. Суджи от 3 02 2014 по делу № 5-25/2014.

[34] Федеральный закон от 25.07.2011 № 261-ФЗ «О внесении изменений в Федеральный закон «О персональных данных» // СЗ РФ. 2011. № 31. Ст. 4701.

[35] General Data Protection Regulation № 2016/679 // URL: http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf (дата обращения: 18.02.2017).

[36] Directive № 2016/680 // URL: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&from=EN (дата обращения 18.02.2017)

Горелишвили Д. Постатейный комментарий к проекту Закона России «О персональных данных» // URL: http://www.kongord.ru/Index/A_tma_05/DGorpersdatcom.html (дата обращения: 16.07.2016)

Покаместова Е.Ю. Правовая защита конфиденциальности персональных данных несовершеннолетних: дис. … к.ю.н. Воронеж, 2006. 204 с.

Рассолов И.М. Информационное право: учебник для магистров. М.: Юрайт, 2012. 444 с.

Cooper D. Re-defining «personal data» — can the opinion live up to the hype? // Data Protection Ireland. 2016. Vol. 10, issue 6, pp. 7–10.

Gkoulalas-Divanis A. Medical Data Privacy Handbook. Berlin: Springer, 2015. 832 p.

Gregory M. Security and the Networked Society. London: Springer, 2013. 289 p.

Black E. IBM and the Holocaust: the Strategic Alliance between Nazi Germany and America's Most Powerful Corporation. New York: Dialog Press, 2012. 532 p.

Kindt E. Privacy and Data Protection Issues of Biometric Applications. Netherlands: Springer, 2013. 975 p.

Kittichaisaree K. Public International Law of Cyberspace. Bern: Springer, 2017. 376 p.

McCullagh K. Data Sensitivity: Proposals for Resolving the Conundrum // Journal of International Commercial Law and Technology. 2007. Vol. 2. Issue 4. P. 197–201.

Mordini E. Second Generation Biometrics: The Ethical, Legal and Social Context. New York: Springer, 2012. 354 p.

Simits S. Revisiting Sensitive Data // URL: https://www.coe.int/t/dghl/standardsetting/dataprotection/Reports/Report_Simitis_1999.pdf (дата обращения: 17.07.2016)

Yue Liu N. Bio-Privacy: Privacy Regulations and the Challenge of Biometrics. New York: Routledge, 2012. 292 p.

Vermeulen G., De Bondt V. Justice, Home Affairs and Security: European and International Institutional and Policy Development. Utrecht: Maklu Publishers, 2017. 298 p.

Peculiarities of Legal Regulating Biometric Personal Data

Maxim Krivogin

Postgraduate Student, International Laboratory for Information Technology and Intellectual Property Law, National Research University Higher School of Economics. Address: 20 Myasnitskaya Str., Moscow 101000, Russia. E-mail: mkrivogin@yandex.ru.

Abstract

Article analyzes the problem of correlation of legal regulation of biometric and sensitive categories of personal data. The author proposes a number of distinctive criteria, enabling to distinct between the categories. The paper also presents the problem of possibility of processing biometric personal data which was made publicly available by data subject. The author analyzes Russian and foreign legal doctrine, statutory acts, Russian decrees of the court in the field of legal regulation of special and biometric categories of personal data. A comparison is made between the list of information contained in special and biometric category of personal data and the possibility of processing such data without data subject's knowledge. The analysis shows that although there are many approaches in legal doctrine and legislation of foreign countries of regulation of biometric personal data, introduction to the Russian legislation special regulation of this type of personal data is expedient. The main distinction between biometric and special category of personal data, in addition to various preconditions of their introduction to the legislation — prohibition of discrimination and restriction of identification of data subject, it is also a list of cases, when data controller is able to process personal data without subject's consent. Inadmissibility of the processing of biometric personal data which were made publicly available provides the possibility to protect information which spread couldn't be exercised in appropriate way. Introduction of subjective (goal) approach of biometric personal data processing provides possibility to make more appropriate distinction between different types of personal data. Information about person would be treated as biometric personal data if it is used by the data controller for the identification of person. Application of such approach nowadays allows to take into consideration interests of subject and controller of personal data.

Keywords

personal data; types of personal data; biometric; special; publicly available; European Union, subjective approach, objective approach.

Citation: Krivogin M.S. (2017) Peculiarities of Legal Regulating Biometric Personal Data. *Pravo. Zhurnal Vysshey shkoly ekonomiki*, no 2, pp. 80–89 (in Russian)

DOI: 10.17323/2072-8166.2017.2.80.89

References

Black E. (2012) *IBM and Holocaust: Strategic Alliance between Nazi Germany and America's Most Powerful Corporation*. N.Y.: Dialog Press, 532 p.

Cooper D. (2016) Re-defining Personal Data — Can the Opinion Live up to the Hype? *Data Protection Ireland*, vol. 3, issue 6, pp. 7–10.

Gkoulalas-Divanis A. (2015) *Medical Data Privacy Handbook*. Berlin: Springer, 832 p.

Goreshvili D. (2016) Postateynyy kommentariy k proyektu Zakona Rossii «O personalnykh dannykh [Commentary to the Law on Personal Data]. Available at: http: // www.kongord.ru/Index/A_tma_05/DGorpersdatcom.html (accessed: 16.07.2016)

Gregory M. (2013) *Security and the Networked Society*. London: Springer, 289 p.

Kindt E. (2012) *Privacy and Data Protection Issues of Biometric Applications.* Leyden: Springer, 975 p.

Kittichaisaree K. (2017) *Public International Law of Cyberspace*. Bern: Springer, 2017. 376 p.

McCullagh K. (2007) Data Sensitivity: Proposals for Resolving the Conundrum. *Journal of International Commercial Law and Technology*, vol. 2, issue 4, pp. 197–201.

Mordini E. (2012) *Second Generation Biometrics: The Ethical, Legal and Social Context*. New York: Norton, 354 p.

Pokamestova E. (2006) *Pravovaya zashchita konfidentsialnosti personalnykh dannykh nesovershennoletnikh:* Diss. Cand. Yurid. Nauk [Legal Protection of Confidentiality of Personal Data Covering Minors. Candidate of Juridical Sciences Dissertation]. Voronezh, 204 p.

Rassolov I. (2012) *Informatsionnoe pravo: uchebnik* [Information Law: Textbook]. Moscow: Yurayt, 444 p. (in Russian).

Simitis S. Revisiting Sensitive Data (1999). Available at: https: //www.coe.int/t/dghl/standardsetting/dataprotection/Reports/Report_Simitis_1999.pdf (accessed: 17.07.2016)

Velder I. (2006) Sistema pravovoy zashchity personalnykh dannykh v Evropeyskom Soyuze: Diss. Cand. Yurid. Nauk [System of Legal Protection of Personal Data in the European Union. Candidate of Juridical Sciences Dissertation]. Kazan, 165 p. (in Russian)

Vermeulen G., De Bondt V. (2017) *Justice, Home Affairs and Security: European and International Institutional and Policy Development.* Utrecht: Maklu Publishers, 298 p.

Yue Liu N. (2012) *Bio-Privacy: Privacy Regulations and the Challenge of Biometrics*. N.Y.: Routledge, 292 p.